ACEEE Int. J. on Network Security , Vol. 4, No. 1, July 2013

Utilizing Data Mining Approches in the Detection of Intrusion in IPv6 Network: Review & Analysis

Redhwan M. A. Saad[1], Selvakumar Manickam[2], Sureswaran Ramadass[3]
[1,2,3]National Advanced IPv6 Centre (NAv6), USM, Pulau Penang, Malaysia.
[1]redhwan@nav6.usm.my, [2]selva@nav6.usm.my, [3]sures@nav6.usm.my

Abstract –**The development of Internet protocols are greatly needed as the network security becomes one of the most important issues. This brings the need to develop IPv4 into IPv6 in order to proceed towards increasing the network capacity.**

Now Intruders are considered as one of the most serious threats to the internet security. Data mining techniques have been successfully utilized in many applications. Many research projects have applied data mining techniques to intrusion detection. Furthermore different types of data mining algorithms are very much useful to intrusion detection such as Classification, Link Analysis and Sequence Analysis.

Moreover, one of the major challenges in securing fast networks is the online detection of suspicious anomalies in network traffic pattern. Most of the current security solutions failed to perform the security task in online mode because of the time needed to capture the packets and making decision about it.

Practically, this study provides alliterative survey for the enhancement associated with IPv6 in terms of its security related functions. It is worthy mentioned that this study is concurred with the data mining approaches that have been used to detect intrusions.

Keywords: **Network Security, IPv6 Security, Intrusion Detection, Denial of Service, Data mining.**

I. Introduction

Intrusion detection system (IDS) is considered as a type of security management system for computers and networks. An IDS inspects all inbound and outbound network activity and identifies patterns that may indicate a network or system detects attack from someone attempting to break into or compromise a system[1].

One of the major challenges in the security management of fast networks is the detection of suspicious anomalies in network traffic patterns because of Distributed Denial of Service (DDoS) attacks or worm propagation [2] A secure network should involve the following:

- Data confidentiality: Data can be transferred through the network and it should be available only for the properly authorized users.
- Data availability: The network should be flexible to Denial of Service attacks.
- Data integrity: Data should retain their integrity starting from the moment of transmission to the moment they are actually received. Corruption or data loss is not accepted either from random events or malicious activity.

The use of the IPv6 protocol brings new demands for typical network protecting mechanisms.

The rest of this work is a survey of intrusion detection in IPv6 networks that is based on data mining techniques which have been utilized in IDSs and is organized as follows: In Section 2, a short classification of IPv6 security issue is presented, which contains subsections as following: In subsection 1, the denial of service attack is discussed. In subsection 2, the previous studies of Distributed Denial of Service (DDoS) attack are reviewed. In subsection 3, a survey of malware attacks in IPv6 Network is presented. In subsection 4, studies of intrusion

detection models for IPv6 network are also presented. In subsection 5, a survey research in IPv6 Address Security is also discussed. In Section 3, the various data mining techniques that have been employed in IDSs by various researchers are discussed and in Section 4, a conclusion is drown, while in Section5, the future work on data mining to intrusion detection in IPv6 networks is proposed.

II. IPv6 security issues

As with any new technology, the initial phases of IPv6 implementation are bound to be exploited by cybercriminals. From a security point of view, the new IPv6 protocol stack represents a considerable advance in relation to the old IPv4 stack. However, in spite of its numberless virtues, IPv6 still continues to be by far vulnerable. In this paper we are going to review a number of the areas of IPv6 where security continues to be a significant issue.

A. Denial of Service in IPv6 Network

One of the major challenges in the fast networks security management is the detection of suspicious anomalies in network traffic patterns because of Distributed Denial of Service (DDoS) attacks. A distributed denial of service attack DDoS only differs with DoS from the method. A DoS is made from a system or network while a DDoS attack is organized to happen simultaneously from a large number of systems or networks[3] as illustrated in figure 1.

The denial of service attack is one of the most significant threats in the IPv4 and IPv6 networks. These attacks consume the network bandwidth and computational resources of the victim and the other users on the same network. The denial of service attack, generated by utilizing the vulnerabilities in the network protocols, affect the performance of the victim as well as the other hosts sharing the network [4]. In recent time [5], it was proposed that an automatic model can be used to analyze the denial of service attacks in security protocol, so Meng protocol can be proved with a mechanized proof tool (ProVerif).

DOI: 01.IJNS.4.1.1382

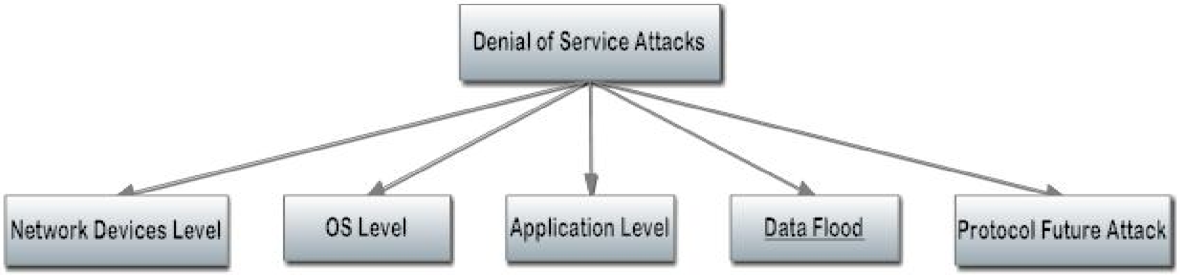

Figure 1. Classification of DoS attacks

B. Distributed Denial of Service in IPv6 Network

According to WWW FAQ concerning the security issues[6], a Distributed Denial of Service (DDoS) attack uses many computers to launch a coordinated DoS attack against one or more targets. Denial of service attacks and distributed denial of service attacks have become the network of one of the main critical problems. According to [4], they proposed a sequential method to detect DDoS attack fast which captures increasing deviations from a normal behavior at times.

As stated in previous research, it has been found that although IPSec provides security for IPv6 network, there is no security at absolute range. Thus, the actual network (SSL/ TTL) flow detection and other network technology should be merged together to protect attacks or potential threats [7].

C. Malware Attacks in IPv6 Network

The number of IPv6 attacks is rather small. As can be noticed, a broader adoption to IPv6, it is more likely to increase in attacks in addition to a larger focus from attackers. Recently, researchers have investigated some possible methods to unfold worms in IPv6 network. One of these methods has been suggested [8]. It has been found that using analysis and simulation may spread P2P-based worms in an IPv6 internet. Findings show that those worms can spread faster and effective in the IPv6 Internet. Consequently, future IPv6 networks have to be compelled to shore the protection of P2P application to prevent the spread of such worms. Based on the practice conducted by [9], there are three scanning strategies used to investigate the worm propagation in IPv6 network in local and wide-area topology, where scanning time is considered as the one of the most significant factors in worm propagation. In addition, IPv6 supports the network security through providing greater security against random scanning worms based on a very sparse address space. Hence, [10] proposed a method called Worm6 used to investigate the worm propagation in IPv6, where these layers have different functions.

D. Intrusion Detection Models for IPv6 Network

Unavoidably, IPv6 will replace the IPv4 as the next generation of the Internet Protocol. Despite IPv6 has better security than IPv4, there are still some security issues. So the significant of IDS for IPv6 networks seem to a critical problem.

An intrusion detection system (IDS) inspects all inbound and outbound network activity and identifies patterns that may indicate a network or system detects attack from someone attempting to break into or compromise a system. IDS has two main intrusion detection techniques anomaly detection and misuse detection. The anomaly detection technique determines the abnormality by measuring the distance between the suspicious activities and the norm based on a chosen threshold. The misuse detection technique looks for a malicious signature or pattern depending on a set of rules or signatures to detect intrusive behavior. The main different between these two IDSs is that the misuse systems cannot detect a novel attacks but it has a lower rate of false alerts. The anomaly models detect the new attacks but they have a higher rate of false alert [11-13]. The general IDS overview in real time is depicted in Figure.2

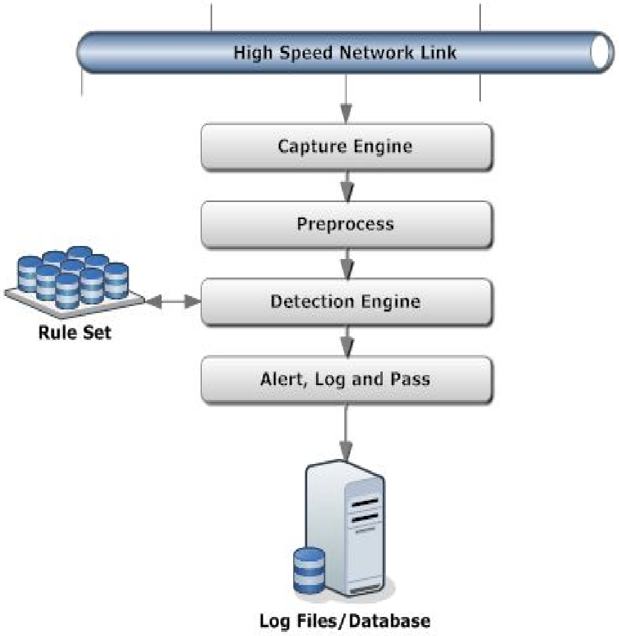

Figure 2. Intrusion Detection Systems Architecture

According to [14], the firewall based on IPv6 can be utilized and configured in networking. The authors also mentioned that distributed intelligent technology can be considered as good tool for the firewall system as a whole. An improved association rule of discovering system under IPv6 network has been studied by [15, 16].

The proposed method presented an intrusion detection model realization for IPv6 network; the proposed strategy for the system revealed good experimental results and improved the base Apriori algorithm and optimization which

DOI: 01.IJNS.4.1.1382

makes association rule mining techniques applicable to IPv6 network. [17] recommended that security mechanisms should be implemented for intrusion detection and packet filtering (firewalls) to improve protection in the IPv6 networks. The mechanisms were carried out to improve IPv6 network security to filter internal-use IPv6 addresses at the edge routers in order to avoid various reconnaissance attacks.

In terms of practice of intrusion detection system on the IPv6 transition mechanism, [18] developed the mechanism with IDS using tunneling mechanism, where IPv6 is expected to discover new resource.

E. IPv6 Address Security

Network operators can provide higher service for every user with fine granularity source address filtered by protecting them from threats and tracing back the malicious host readily. [19] observes that granularity source address validation has been deployed in various campus networks. In addition, the Duplicate Address Detection (DAD) algorithm is used to ensure that all configured addresses nodes on link are trustworthy. As [20] comment, a pull model DAD is used to improve a mechanism to secure DAD in IPv6.

For the security needs of the next generation Internet (IPv6), and based on the [21] NetFlow, data can be gathered to design a traffic monitoring system to realize overall statistical analysis of the network traffic and thus alerts the system of the abnormal traffic. To find the MAC address in IPv6 networks, IPv6 uses Network Discovery Protocol (NDP). In IPv6 NDP [22], demonstrated a technique for detecting spoofing neighboring solicitation and advertisement attacks.

F. Flooding Attack Using ICMPv6

One of the most frequent attack types present in IPv4 networks is a flooding attack. It connotes flooding a network device (e.g. a router) or a host with large amounts of network traffic. A targeted device is unable to process such large amount of network traffic and becomes unavailable or out of service. A flooding attack can be local or a distributed denial of service attack (DDoS), when the targeted network device is being flooded by network traffic from many hosts simultaneously. This type of attack can also affect the IPv6 networks, because the basic principles of the flooding attack remain the same [23-26].

DDoS flooding attacks are often launched in two type of attacks: direct attacks and reflector attacks. In direct attacks, the attacker directly sends a flood of bogus packets toward the victim through the zombie machines. Direct DDoS attacks are classified into two categories: application-layer DDoS attacks and network-layer DDoS attacks. Application-layer DDoS attacks encompass: HTTP flood, HTTPS flood, FTP flood, etc. Network-layer DDoS attacks encompass: TCP flood, UDP flood, ICMP flood and SYN flood. In reflector attacks, the attacker sends request messages to reflector machines through zombie machines, spoofing the source IP address of the victim server. As a result, the reflector machines send their replies to the given address causing packet flooding at that site which is the victim server. The well-known reflector attacks are ICMP ECHO reply flood, SYN ACK (RST) flood, DNS flood, Smurf attack and Fraggle attack [27]. Figure 3 shows direct DDoS and reflector DDoS attacks.

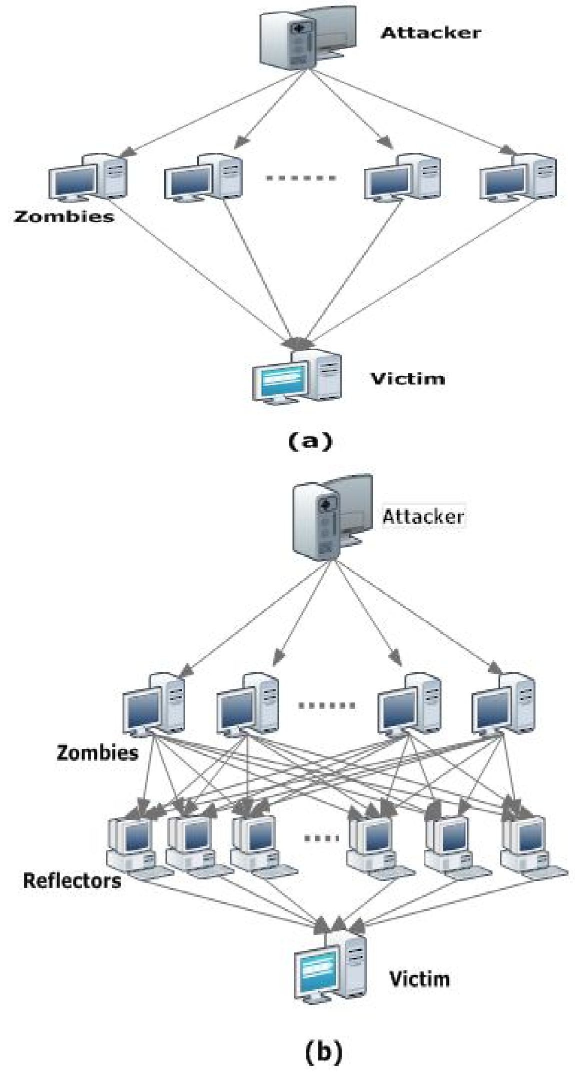

Figure 3. The architecture of flooding DDoS attacks: (a) direct, (b) reflector.

III. Techniques of Anomaly-Based Intrusion Detection System

In this section we review different techniques of Anomaly based IDS. The most important are Data mining based detection, Statistical anomaly detection, Knowledge based detection, and Machine learning based detection. The complete classification of ABIDS is shown in the Figure 4.

As IDS can only detect known attacks, but it cannot detect insider attacks, the better solution for an IDS can be Data Mining at its core is “pattern finding” and is defined as “the process of extracting useful and previously unnoticed models or patterns from large data stores”. Data mining is the latest introduced technology of intrusion detection. In addition, data-mining process tends to reduce the amount of data that must be retained for historical comparisons of network activity, creating data that is more meaningful to anomaly detection [28-31].

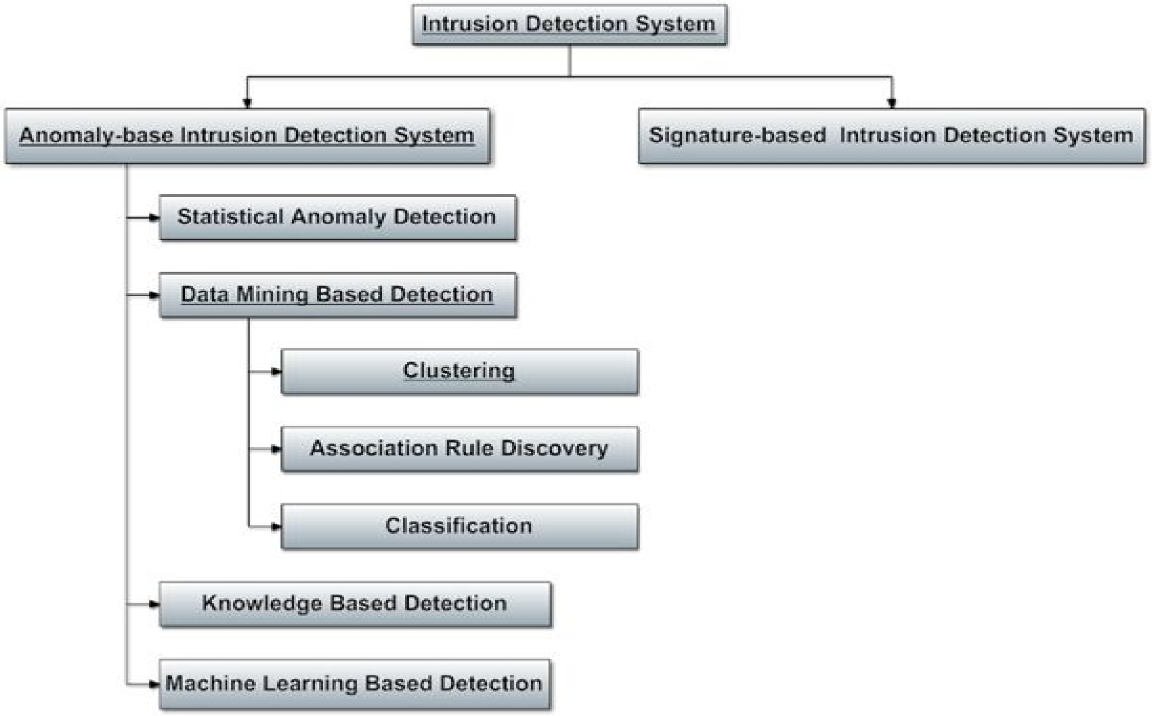
Intrusion Detection System
Anomaly-base Intrusion Detection System
Signature-based Intrusion Detection System
Statistical Anomaly Detection
Data Mining Based Detection
Clustering
Association Rule Discovery
Classification
Knowledge Based Detection
Machine Learning Based Detection

Figure 4. Taxonomy of Anomaly based Intrusion Detection System

IV. Employed Data Mining Techniques In IDSS

The techniques of different data mining are categorized based on their functions, preference criterion, representation and algorithms [32]. Additionally, data mining system provide the means to perform data summarization and visualization, for aiding the security analyst and identifying areas of interest. Common representations for data mining techniques include rules, decision trees, linear and non-linear functions including neural networks, based examples and probability models [32]. Furthermore, it has been suggested that a novel data mining approach, (i.e., Bi-clustering) potentially contributes to creating a better and more effective way of Intrusion Detection Systems[33].

Security products such as Firewalls and Network Intrusion Detection Systems have less support for the IPv6 protocols than for their IPv4 counterparts either in terms of features or in terms of performance [34]

An intrusion detection algorithm and its architecture (two-layered, global central layer and a local layer, together performing data collection, analysis and response), based on data mining and useful in real time for network security, is proposed be HAZEM M. EL-BAKRY et al [35]. By filtering out the known traffic behavior (intrusive and normal) this IDS focuses on analysis on unknown data thereby reducing false alarm rates.

Tich Phuoc Tran et al [36] proposed an approach called “A Multi-Expert Classification Frameworkwith Transferable Voting for Intrusion Detection”. This model, aimed to improve the strategies to detect different anomalies and intrusions emphasized on different attribute selection strategies, defined a new multi expert classification system to test the limits in accuracy and robustness in existing systems and showed that some learning algorithms that use certain set of features can provide superior detection capability for a given attack category. A set of five local classifiers, created to detect five different classes including Normal, Probe, DoS, U2R and R2L and outputs from these experts are then integrated by different voting methods. Finally concluded that a) the weighted voting strategies outperform simple majority voting, b) with Transferable voting approach, the model achieved noticeable performance improvement compared with other conventional techniques, in terms of detection accuracy and system robustness, misclassification cost and processing overheads for “unknown” instances. This may not be an ultimate choice for security, but is effective on different situations.

V. Conclusion

The main purpose of this paper is to explore the most recent literature which discussed the intrusion detection system based on data mining approaches. Based on literature review, it is found that data mining algorithms such as Classification, Link Analysis, and Sequence Analysis are very helpful in intrusion detection. Recently, many networks begin with the deployment of the ipv6 after the exhaustion of the ipv4 addresses networks. So, as with any new technology, the initial stages of IPv6 implementation are bound to be targeted by cybercriminals.

Denial of service attacks and distributed denial of service attacks have become the network for one of the main critical problems. Network operators can provide higher service for every user with fine granularity source address filtered by protecting them from threats and tracing back the malicious host readily.

VI. Future Work

The future work will investigate more advanced data mining techniques for effective and efficient detection of intrusion in IPv6 network. The Hybrid Intelligent System will be considered to enhance the intrusion detection in the IPv6 network as it has the capability of solving most of the unsolved problem in the field of Network Intrusion Detection

Acknowledgements

The authors would like to thank the anonymous reviewers for their valuable comments and suggestions to improve the quality of the paper. This original research was proudly supported by the RUT grant of University Science Malaysia (Grant No. 1001/PANY/857001).

References

[1] (2012). Intrusion detection system. Available: *http://www.webopedia.com/TERM/I/intrusion_detection _system .html*

[2] C. Douligeris and A. Mitrokotsa, "DDoS attacks and defense mechanisms: Classification and state-of-the-art," Computer Networks, vol. 44, pp. 643-666, 2004.

[3] L. P. Tixteco, et al., "DoS Attacks Flood Techniques," International Journal, vol. 3, 2012.

[4] S. Meenakshi and S. K. Srivatsa, "A Distributed Framework with less False Positive Ratio Against Distributed Denial of Service Attack.," Information Technology Journal, p. 6, 2007.

[5] W. Huang and B. Meng, "Automated proof of resistance of denial of service attacks in remote internet voting protocol with extended applied Pi calculus," Information Technology Journal, vol. 10, pp. 1468-1483, 2011.

[6] L. D. Stein and J. Stewart, *World Wide Web Security FAQ* vol. 3.1.2: Lincoln D. Stein., 2002.

[7] W. Hui, *et al.*, "DDoS/DoS Attacks and Safety Analysis of IPv6 Campus Network: Security Research under IPv6 Campus Network," in *Internet Technology and Applications (iTAP), 2011 International Conference on*, 2011, pp. 1-4.

[8] W. Yang, *et al.*, "The Effect of P2P-Based Worm Propagation in an IPv6 Internet," *Procedia Engineering,* vol. 15, pp. 3637-3641, 2011.

[9] J. Li, *et al.*, "The research and analysis of worm scanning strategies in IPv6 network," in *Network Operations and Management Symposium (APNOMS), 2011 13th Asia-Pacific*, 2011, pp. 1-4.

[10] L. Zhaowen, *et al.*, "The analysis of Internet worm modeling in IPv4 and IPv6 networks," in *Broadband Network and Multimedia Technology (IC-BNMT), 2010 3rd IEEE International Conference on*, 2010, pp. 738-743.

[11] O. Abouabdalla, *et al.*, "False positive reduction in intrusion detection system: A survey," 2009, pp. 463-466.

[12] Y. Liao and V. R. Vemuri, "Use of K-nearest neighbor classifier for intrusion detection," *Computers & Security,* vol. 21, pp. 439-448, 2002.

[13] A. Alharby and H. Imai, "IDS false alarm reduction using continuous and discontinuous patterns," 2005, pp. 423-442.

[14] Q. Ma, *et al.*, "Design and Implementation of Distributed Intelligent Firewall Based on IPv6," pp. 703-707, 2009.

[15] J. Chen and X. Chen, "Intrusion Detection System Research Based on Data Mining for IPv6," in *Information Technology and Applications (IFITA), 2010 International Forum on*, 2010, pp. 384-388.

[16] Z. Liu and Y. Lai, "A Data Mining Framework for Building Intrusion Detection Models Based on IPv6.." vol. 5576, J. Park, *et al.*, Eds., ed: Springer Berlin / Heidelberg, 2009, pp. 608-618.

[17] D. Žagar, *et al.*, "Security aspects in IPv6 networks – implementation and testing," *Computers &amp; Electrical Engineering,* vol. 33, pp. 425-437, 2007.

[18] N. Bahaman, *et al.*, "Implementation of IPv6 network testbed: Intrusion detection system on transition mechanism," *Journal of Applied Sciences,* vol. 11, pp. 118-124, 2011.

[19] L. Fuliang, *et al.*, "Investigating the efficiency of fine granularity source address validation in IPv6 networks," in *Network Operations and Management Symposium (APNOMS), 2011 13th Asia-Pacific*, 2011, pp. 1-8.

[20] Y. Guang, *et al.*, "A pull model IPv6 Duplicate Address Detection," in *Local Computer Networks (LCN), 2010 IEEE 35th Conference on*, 2010, pp. 372-375.

[21] L. Yuhui, *et al.*, "Next Generation Internet Traffic Monitoring System Based on NetFlow," in *Intelligent System Design and Engineering Application (ISDEA), 2010 International Conference on*, 2010, pp. 1006-1009.

[22] F. A. Barbhuiya, *et al.*, "Detection of neighbor solicitation and advertisement spoofing in IPv6 neighbor discovery protocol," 2011, pp. 111-118.

[23] D. Zagar and K. Grgic, "IPv6 security threats and possible solutions," 2006, pp. 1-7.

[24] R. Radhakrishnan, *et al.*, "Security issues in IPv6," 2007, pp. 110-110.

[25] X. Yang, *et al.*, "Typical DoS/DDoS Threats under IPv6," 2007, pp. 55-55.

[26] A. R. Choudhary, "In-depth analysis of IPv6 security posture," 2009, pp. 1-7.

[27] H. Beitollahi and G. Deconinck, "Analyzing well-known countermeasures against distributed denial of service attacks," *Computer Communications,* vol. 35, pp. 1312-1332, 2012.

[28] I. H. Witten, *et al.*, *Data Mining: Practical Machine Learning Tools and Techniques: Practical Machine Learning Tools and Techniques*: Morgan Kaufmann, 2011.

[29] C. Romero, *et al.*, "Data mining in course management systems: Moodle case study and tutorial," *Computers & Education,* vol. 51, pp. 368-384, 2008.

[30] M. S. Narayana, *et al.*, "Data Mining Machine Learning Techniques–A Study on Abnormal Anomaly Detection System," *International Journal of Computer Science and Telecommunications,* vol. 2, 2011.

[31] J. E. Dickerson and J. A. Dickerson, "Fuzzy network profiling for intrusion detection," in *Fuzzy Information Processing Society, 2000. NAFIPS. 19th International Conference of the North American*, 2000, pp. 301-306.

[32] U. Fayyad, *et al.*, "The KDD Process for Extracting Useful Knowledge from Volumes of Data," *Communications of the ACM,* vol. 39, pp. 27-34, 1996.

[33] G. Mohammed Nazer and A. Arul Lawrence Selvakumar, "Intelligent data mining techniques for intrusion detection models on network," *European Journal of Scientific Research,* vol. 71, pp. 36-45, 2012.

[34] F. Gont, "Recent advances in IPv6 Security," *IETF Internet Draft,* 2012.

[35] H. M. El-Bakry and N. Mastorakis, "A real-time intrusion detection algorithm for network security," *WSEAS Transactions on Communications,* vol. 7, pp. 1222-1228, 2008.